IN THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CYNTHIA REDD, individually and on behalf of all others similarly situated, Plaintiff, v. AMAZON WEB SERVICES, INC., Defendant.	Case No. 1:22-cv-06779 Hon. Elaine E. Bucklo

AMAZON WEB SERVICES, INC.'S RULE 12(b)(2) AND RULE 12(b)(6) MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

OTHER AUTHORITIES

INTRODUCTION

Plaintiff Cynthia Redd seeks to expand the Illinois Biometric Information Privacy Act ("BIPA") far beyond what its authors could have possibly intended. Her claims should be dismissed in their entirety and with prejudice under Federal Rule of Civil Procedure ("Rule") 12(b)(2) or, in the alternative, under Rule 12(b)(6).[1]

Ms. Redd signed up for Wonolo, a mobile application that connects job seekers with potential employers. She claims Wonolo verified her identity by comparing photos of her face—specifically, photos she provided to Wonolo when she created her Wonolo account and photos she provided to Wonolo when she arrived at job sites. She further alleges that Wonolo compared her photos using Rekognition, a cloud-based software service offered by Amazon Web Services, Inc. ("AWS") to its customers. To be clear, Ms. Redd does not allege that she interacted with AWS in any way, or that AWS was even aware of her use of Wonolo. Nevertheless, Ms. Redd seeks to hold AWS liable on the theory that AWS—not Wonolo—improperly collected, possessed, disclosed, and profited from biometric data about her face.

Ms. Redd's claims fail on multiple levels. For starters, this Court lacks personal jurisdiction over AWS because Ms. Redd has not alleged and cannot allege that her claims arise from any Illinois-based conduct by AWS. In addition, Ms. Redd comes nowhere near alleging the essential elements of her claims. And, more fundamentally, her novel attempt to sweep into BIPA's scope back-end cloud-service providers like AWS is inconsistent with any rational reading of the law. Finally, even if Ms. Redd could overcome those hurdles, her claims would still fail because AWS complied with BIPA by contractually requiring its customers, including Wonolo, to comply with the law. As multiple courts have confirmed, nothing more is required.

[1] This is the third BIPA lawsuit filed by Ms. Redd. In another case, Ms. Redd claims Amazon collected her biometric data without her consent when it conducted temperature screenings designed to protect its employees from COVID-19. *See Redd v. Amazon.com, Inc.*, No. 1:20-cv-06485 (N.D. Ill.) (Dkt. 55). Amazon has moved for summary judgment in that case because, among other things, the record shows that Amazon never collected Ms. Redd's biometric data. *See id.* (Dkt. 85). Ms. Redd also sued Wonolo—the same third party at issue in this case—alleging Wonolo violated her rights under BIPA. She voluntarily dismissed that case shortly after Wonolo moved to compel arbitration. *See Redd v. Wonolo, Inc.*, No. 1:22-cv-00292 (N.D. Ill.) (Dkts. 16, 17, 19, 26).

Ms. Redd may or may not have valid claims against Wonolo, the company that (she claims) required her to disclose photos of her face and then analyzed those photos. But she certainly has no claims against AWS, which has no relationship to Ms. Redd and merely acted as a back-end, out-of-state service provider for Wonolo. Ms. Redd's claims should be dismissed.

BACKGROUND

A. The Illinois Biometric Information Privacy Act ("BIPA")

All Ms. Redd's claims arise under BIPA, an Illinois state law that specifically regulates "biometric identifiers" and "biometric information" (collectively, "biometric data").[2] BIPA does not prohibit the collection and use of biometric data. Rather, it imposes obligations on private entities if they engage in certain activities with respect to biometric data. As relevant here, Section 15(b) of BIPA requires companies that "collect . . . or otherwise obtain" biometric data to provide notice and obtain consent before doing so. 740 ILCS 14/15(b). Other sections of BIPA, in turn, require companies "in possession" of biometric data to develop and comply with "a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying" biometric data, *id*. 14/15(a) ("Section 15(a)"); refrain from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from" biometric data, *id.* 14/15(c) ("Section 15(c)"); and refrain from "disclos[ing], redisclos[ing], or otherwise disseminat[ing]" biometric data unless certain exceptions apply, *id.* 14/15(d) ("Section 15(d)").

BIPA's penalties are harsh. It grants a private right of action for actual damages or, alternatively, liquidated damages of $1,000 per negligent violation or $5,000 per intentional or reckless violation. *See id*. 14/20(1), (2). A prevailing party also may recover attorneys' fees and costs. *See id*. 14/20(3). The potential for enormous recoveries has inspired a wave of more than 1,500 putative class actions under BIPA in recent years. *See* Declaration of Ryan Spear ("Spear Decl.") ¶ 2; *see also id*., Ex. A (U.S. Chamber of Commerce Institute for Legal Reform,

[2] By referring to "biometric data" throughout this motion, AWS does not concede that it collected, possessed, profited from, or disclosed any data regarding Ms. Redd. Further, AWS specifically reserves the right to argue, at the appropriate time, that even if it did collect, possess, store, profit from, or disclose any data about Ms. Redd, no such data qualifies as "biometric identifiers" or "biometric information" within the meaning of BIPA.

ILR Briefly, *A Bad Match: Illinois and the Biometric Information Privacy Act* 4, 7 (Oct. 2021)) (noting the "exponential growth in BIPA litigation").

B. Amazon Web Services ("AWS"), Rekognition, and Wonolo

AWS is "one of the largest platforms and providers of cloud computing services." Class Action Complaint ("Compl.") ¶ 1 (Dkt. 1-1). "An external cloud platform is storage or software access that is essentially rented from (or outsourced to) a remote public cloud service provider, such as Amazon or Google." *United States v. Cotterman*, 709 F.3d 952, 965 n.12 (9th Cir. 2013) (en banc) (cleaned up). In practical terms, AWS's cloud services allow AWS customers, like Wonolo, to remotely access computer servers and software services provided by AWS to store and process the customers' own data, however they see fit. *See* Compl. ¶ 38.

Rekognition is one of the cloud-based software services that AWS provides to its customers. *See id*. ¶ 4. "Rekognition is an image-recognition technology" that AWS customers can use to analyze images of faces for various purposes. *Id.* For example, AWS customers can use Rekognition to verify their users' identities by comparing photos and generating "similarity scores" reflecting how likely it is that those photos contain images of the same person's face. *See, e.g.*, AWS, Amazon Rekognition FAQs, Face Comparison & Face Recognition, https://aws.amazon.com/rekognition/faqs/?nc=sn&loc=7 (last visited Jan. 17, 2023) (cited at Compl. at 2 n.1) (attached as Exhibit B to the Spear Declaration).[3] AWS makes Rekognition available only to customers who agree to the AWS Customer Agreement. *See* Spear Decl., Ex. C (AWS Customer Agreement) ¶ 1.1. The AWS Customer Agreement, in turn, incorporates the

[3] Ms. Redd cites to AWS's website repeatedly, including to support allegations about how Rekognition works and how it was used by Wonolo. *See, e.g.*, Compl. at 2 n.1; *id*. ¶¶ 4–10, 43. She also specifically alleges that Wonolo "retained AWS" to "host data from its job placement application" and for "software services, including . . . its Rekognition program." *Id*. ¶ 3. Thus, under the incorporation-by-reference doctrine, the Court may consider AWS's website and documents on AWS's website that pertain to those matters, including the AWS Customer Agreement. *See McGoveran v. Amazon Web Servs., Inc.* ("*McGoveran II*"), No. CV 20-1399-LPS, 2021 WL 4502089, at *4 n.3 (D. Del. Sept. 30, 2021) (where, as here, plaintiffs' complaint "cite[d] the AWS website multiple times," court could consider relevant documents on that website). Alternatively, the Court may take judicial notice of the AWS website and documents. *See, e.g.*, *Goplin v. WeConnect, Inc.*, 893 F.3d 488, 491 (7th Cir. 2018); *James v. City of Evanston*, No. 20-CV-00551, 2021 WL 4459508, at *7 n.3 (N.D. Ill. Sept. 29, 2021).

AWS Service Terms, which require Rekognition customers to "provid[e] legally adequate privacy notices to End Users," such as Ms. Redd, and to "obtain[] any necessary consent from such End Users for the processing of" their data. *See id.*, Ex. D (AWS Service Terms) ¶ 50.4. The AWS Customer Agreement also makes clear that data collected by customers belongs to customers, and hence that AWS may not "access or use" customers' content "except as necessary to maintain or provide [AWS] Service Offerings, or as necessary to comply with the law or a binding order of a governmental body." *Id.*, Ex. C (AWS Customer Agreement) ¶ 3.2.

Ms. Redd alleges that Wonolo is one of "millions of customers around the world" who use Rekognition in their own products and services. Compl. ¶ 38. According to Ms. Redd, Wonolo "provides an on-demand web-based staffing platform" that helps job seekers connect with employers. *Id.* ¶ 2. Ms. Redd claims she signed up for Wonolo in May 2020, at which time Wonolo required her to upload a photo of her face via the Wonolo app. *See id.* ¶ 54. Later, Ms. Redd accepted several jobs for "Wonolo's employer-customer locations in Illinois." *Id.* ¶ 55. Each time she did so, Ms. Redd alleges she was required to submit additional photos of herself "at a Wonolo device located at the customer-employer jobsite location." *Id.* ¶ 56. Ms. Redd further alleges that Wonolo entered into a contract with AWS that allowed Wonolo to use Rekognition to (1) "host and store" Ms. Redd's photos and (2) compare those photos to verify her identity while she was using Wonolo's services. *Id.* ¶¶ 3, 39, 41. Importantly, Ms. Redd does not allege that AWS played any role in Wonolo's verification process beyond allowing Wonolo to use Rekognition. Indeed, Ms. Redd does not even allege that AWS knows or could know when Wonolo uses Rekognition to verify the identities of Illinois residents like herself.

C. Ms. Redd's Claims Against AWS

Based solely on Wonolo's use of Rekognition, Ms. Redd now contends that AWS itself violated BIPA in four ways. First, she alleges AWS violated Section 15(a) of BIPA by possessing her biometric data without developing and complying with a publicly available retention schedule for permanently destroying that data. *See id.* ¶¶ 83–91. Second, she alleges AWS violated Section 15(b) of BIPA by collecting her biometric data without providing notice

or obtaining consent. *See id.* ¶¶ 92–101. Third, she alleges AWS violated Section 15(c) of BIPA by using her biometric data to "enhance and train" Rekognition and thereby "profiting" from it. *See id.* ¶¶ 102–10. Fourth, she alleges AWS violated Section 15(d) of BIPA by disclosing her biometric data without her consent. *See id.* ¶¶ 111–19.

Ms. Redd asserts all four claims on behalf of herself and "[a]ll individuals enrolled in the Wonolo application in the State of Illinois who had their facial geometry collected, captured, received, or otherwise obtained, maintained, stored, used or disclosed by AWS during the applicable statutory period." *Id.* at ¶ 73.

ARGUMENT

A. Ms. Redd's Complaint Should Be Dismissed Under Rule 12(b)(2)

As a threshold matter, Ms. Redd's Complaint should be dismissed for lack of personal jurisdiction under Rule 12(b)(2) because she has not alleged, and could not allege, that her claims arise from Illinois-based conduct by AWS.

There are two types of personal jurisdiction: "general or all-purpose jurisdiction," and "specific or case-linked jurisdiction." *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 919 (2011). AWS is not subject to general jurisdiction because AWS is not incorporated in Illinois and is not "essentially at home" in this state. *Id.*; *see also, e.g.*, *McGoveran v. Amazon Web Servs., Inc.* ("*McGoveran I*"), 488 F. Supp. 3d 714, 719 (S.D. Ill. 2020) ("[T]he Supreme Court has identified only two places where a corporation is 'at home': the state of the corporation's principal place of business and the state of its incorporation.").

Thus, for her case to proceed, Ms. Redd must adequately allege facts sufficient to show specific jurisdiction. *See N. Grain Mktg., LLC v. Greving*, 743 F.3d 487, 491–92 (7th Cir. 2014). That means she must allege a strong "affiliation between the forum and the underlying controversy." *Bristol-Myers Squibb Co. v. Superior Court*, 137 S. Ct. 1773, 1780 (2017). In particular, she must plausibly allege that AWS's "suit-related conduct" creates "a substantial connection" with Illinois. *Walden v. Fiore*, 571 U.S. 277, 284 (2014); *see also, e.g.*, *Advanced Tactical Ordnance Sys., LLC v. Real Action Paintball, Inc.*, 751 F.3d 796, 801 (7th Cir. 2014), as

corrected (May 12, 2014) ("The relevant contacts are those that center on the relations among the defendant, the forum, and the litigation."). Put another way, Ms. Redd must allege facts showing that (1) AWS specifically "targeted [Illinois] somehow," and that (2) her claims arise from AWS's efforts to target Illinois. *Id*. at 801, 803; *see also McGoveran I*, 488 F. Supp. 3d at 720 (same; dismissing case against AWS for lack of personal jurisdiction).

Ms. Redd cannot meet those requirements. Nothing in her Complaint suggests AWS "targeted" Illinois in this case. In fact, Ms. Redd does not allege a single significant connection between AWS and Illinois—let alone a significant connection between AWS, Illinois, and *her claims*. To the contrary, Ms. Redd admits that neither AWS nor Wonolo are incorporated or headquartered in Illinois. *See* Compl. ¶¶ 1, 2. And she does not allege that AWS deliberately reached into Illinois to interact with her or other Wonolo users in the state (it did not) or that AWS stored or processed data about her face in data centers or other resources located in Illinois (again, it did not). *See* AWS, Using AWS in the Context of Common Privacy and Data Protection Considerations, https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf (last visited Jan 17, 2023) (attached as Exhibit E to the Spear Declaration).[4]

Instead, Ms. Redd alleges only that she is an Illinois resident; that she used the Wonolo app in Illinois; and that Wonolo entered into a contract with AWS. *See, e.g.*, Compl. ¶¶ 22, 54–55, 39. That is insufficient. As the Seventh Circuit has explained, "there can be no doubt that the plaintiff cannot be the only link between the defendant and the forum." *Advanced Tactical*, 751 F.3d at 802–03 (internal quotation marks and citation omitted). Thus, Ms. Redd's residency in Illinois does not confer personal jurisdiction over AWS. The fact that Ms. Redd used the Wonolo app in Illinois is likewise inadequate because the Supreme Court has "consistently

[4] The Court may consider publicly available documents regarding the location of AWS's data centers under the incorporation-by-reference doctrine, the judicial notice doctrine, or both. *See McGoveran II*, 2021 WL 4502089, at *4 n.3 (considering the same document cited here under the incorporation-by-reference doctrine); *see also supra* n.3.

rejected attempts to [establish personal jurisdiction] by demonstrating contacts between the plaintiff (or third parties) and the forum State." *Walden*, 571 U.S. at 284.

Finally, Ms. Redd's claim that Wonolo contracted with AWS to use Rekognition is also insufficient. *McGoveran I* is instructive. There, plaintiffs argued that AWS was subject to specific personal jurisdiction in Illinois because (1) plaintiffs, who were Illinois residents, interacted with a non-resident company via telephone; (2) plaintiffs' voice data was captured during those interactions; and (3) plaintiffs' voice data was ultimately stored on AWS servers. The court rejected that jurisdiction-by-association theory and dismissed plaintiffs' claims against AWS because, as here, there was no allegation that *AWS itself* targeted Illinois, and because "specific jurisdiction cannot be established through a third party's contacts with the forum state." *McGoveran I*, 488 F. Supp. at 721. This Court should reach the same conclusion.[5]

B. Ms. Redd's Complaint Should Be Dismissed Under Rule 12(b)(6)

Even if Ms. Redd could establish specific jurisdiction, her Complaint should still be dismissed under Rule 12(b)(6) because she cannot allege the essential elements of her claims.

1. Ms. Redd alleges no facts showing that AWS "possessed" her data.

Sections 15(a), (c), and (d) of BIPA apply only to private entities "in possession of" biometric data. 740 ILCS 14/15(a), (c), and (d). But Ms. Redd does not, and cannot, allege any facts showing that AWS possessed her data within the meaning of those provisions.

[5] For similar reasons, Ms. Redd's claims fail under the Illinois extraterritoriality doctrine. BIPA applies only to conduct "occurr[ing] primarily and substantially in Illinois." *Avery v. State Farm Mut. Auto. Ins. Co*., 216 Ill. 2d 100, 187 (2005). Here, Ms. Redd does not plausibly allege that AWS engaged in *any* conduct in Illinois. And she certainly does not allege that AWS's purportedly unlawful conduct occurred "primarily" and "substantially" in Illinois, nor could she. Thus, BIPA simply does not apply. *See Vance v. Amazon.com*, No. 20-cv-1084-JLR, 2022 WL 12306231, at *6–8 (W.D. Wash. Oct. 17, 2022) (dismissing BIPA claims against Amazon on extraterritoriality grounds); *McGoveran II*, 2021 WL 4502089, at *3 (dismissing BIPA claims against AWS on extraterritoriality grounds). The *McGoveran II* court later allowed plaintiffs' claims to proceed because "new allegations [in plaintiffs' amended complaint] rais[ed] at least a plausible inference that [AWS's] alleged misconduct occurred principally and substantially in Illinois," including that AWS "interacted *directly* with Plaintiffs in Illinois." *See McGoveran II*, No. 1:20-cv-01399-SB (D. Del. Feb. 14, 2022) (Dkt. 46) (emphasis added). Ms. Redd, in contrast, does not and cannot allege any direct interactions between her and AWS in Illinois.

BIPA does not define "possession." Courts therefore "assume the legislature intended for it to have its popularly understood meaning." *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019) (citations omitted). "[P]ossession, as ordinarily understood, occurs when a person *has or takes control* of the subject property or *holds the property at his or her disposal*." *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005) (cleaned up) (emphasis added). Thus, to trigger BIPA's "possession" requirements, a defendant must "take control" of biometric data or "hold" that data "at his or her disposal." *Barnett v. Apple Inc.*, 2022 IL App (1st) 220187, ¶¶ 39–43, 2022 WL 17881712, at *6–7 (2022) (dismissing Section 15(a) claim for lack of possession).

Here, Ms. Redd does not allege that AWS controlled or even knew about the data (including photos of her) that Wonolo allegedly uploaded to AWS. Nor could she. The AWS Customer Agreement makes clear that AWS does "not access or use . . . Content [of AWS customers like Wonolo] except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body." Spear Decl., Ex. C (AWS Customer Agreement) ¶ 3.2. And it states, in no uncertain terms, that AWS customers "are solely responsible for the development, content, operation, maintenance, and use of [their] Content." *Id.* ¶ 4.2. Thus, Wonolo "maintain[s] *full control*" of any "content that [it] upload[s] to" AWS's servers, and AWS does "not access or use [the] content for any purpose without [Wonolo's] agreement." Spear Decl., Ex. F at 1–2 (AWS Data Privacy FAQ) (emphasis added).

Ms. Redd's allegations are entirely consistent with the AWS Customer Agreement. She claims that *Wonolo* "required [her] to scan her facial geometry," Compl. ¶ 56; that *Wonolo* "compare[d] Wonolo workers' images" to verify their identities, *id.* ¶ 8; and that *Wonolo* determined how and where to store and use the data generated by Ms. Redd's use of Wonolo's app, *see id.* ¶ 3. Nothing in Ms. Redd's Complaint suggests AWS had any knowledge of those alleged events, or that AWS exercised, or could have exercised, any control over the data. In short, it defies common sense—and the text of BIPA—to say that AWS "possessed" Ms. Redd's data when it was subject to Wonolo's exclusive "dominion and control" at all times. *See Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 962, 968–69 (N.D. Ill. 2020)

(dismissing Section 15(a) claim against defendant who allegedly "stored" biometric data on behalf of another party because allegations of mere storage did not amount to a "form of control" or show that the defendant "could freely access the data").[6]

Further, Ms. Redd's attempt to stretch the concept of "possession" to encompass AWS invites absurd results. *See, e.g.*, *Solon v. Midwest Med. Recs. Ass'n*, 236 Ill. 2d 433, 441 (2010) (when interpreting statutes, courts must "presume that the legislature did not intend absurd, inconvenient, or unjust consequences"). When Section 15(a) applies, it requires a private entity to publish a deletion schedule *and* to "permanently destroy[]" biometric data "when the initial purpose for collecting or obtaining" the data "has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a). Ms. Redd does not explain how AWS could meet those demands in this context, nor could she. As noted above, AWS is generally prohibited from "access[ing] or us[ing]" its customers' data. Spear Decl., Ex. C (AWS Customer Agreement) ¶ 3.2. As a result, AWS does not know whether (much less when) customers like Wonolo upload *biometric* data to their AWS account. Nor does AWS know whether (much less when) its customers upload biometric data from *Illinois residents*. Thus, AWS would not even be able to determine when BIPA might apply under Ms. Redd's reading of the law. It follows that AWS could not publish a Section 15(a) policy accurately reflecting how and when any BIPA-covered data would be deleted, much less determine when that data should be deleted. And, of course, if AWS were to delete end users' data contrary to the wishes of AWS customers, then AWS could disrupt its customers' businesses and incur liability to its customers under the parties' contracts and other authorities.[7]

[6] The *Heard* court later allowed the plaintiff's Section 15(a) claim to survive a second motion to dismiss. *See Heard*, 524 F. Supp. 3d 840. But the court did so only after the plaintiff amended the complaint to add plausible allegations that the defendant "exercise[d] some form of control" over the plaintiff's data. Ms. Redd's Complaint includes no such allegations.

[7] For these and other reasons, AWS contractually requires customers who use Rekognition to "notify[] [AWS] in the event that any [customer content] stored by [Rekognition] must be deleted under applicable law." Spear Decl., Ex. D (AWS Service Terms) ¶ 50.4.

In short, endorsing Ms. Redd's reading of "possession" would, at the very least, require AWS to determine the residency of each of Wonolo's end users, as well as the types of data that Wonolo collected from those end users. Even if AWS was allowed to access its customers' data for such purposes (and it is not), it has no way to conduct that sort of forensic analysis. Ms. Redd's claims under Sections 15(a), (c), and (d) therefore collapse into incoherence.[8]

2. Ms. Redd alleges no facts showing that AWS "collected" her data.

Ms. Redd's Section 15(b) claim fails for similar reasons. Section 15(b) applies only to private entities that "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data. 740 ILCS 14/15(b). (For brevity, AWS uses the word "collect" to encompass all the relevant terms.) But Ms. Redd does not, and cannot, allege that AWS collected her biometric data within the meaning of Section 15(b).

BIPA does not define Section 15(b)'s operative terms. However, because the legislature included the term "possession" in Section 15(a) but not in Section 15(b), it follows that mere "possession of biometric data is insufficient to trigger Section 15(b)'s requirements." *Heard*, 440 F. Supp. 3d at 965 (collecting cases). Further, the legislature must have meant to distinguish "between possessing and collecting biometric information." *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 285–86 (N.D. Ill. 2019). Thus, courts have held that collection requires "something more" than mere possession. *Jacobs v. Hanwha Techwin Am., Inc.*, No. 21 C 866, 2021 WL 3172967, at *2 (July 27, 2021). And that "something more" is an "affirmative act" or

[8] Ms. Redd's novel interpretation of "possession" would lead to untenable results for large swaths of the economy, not just AWS. Under Ms. Redd's reading, other companies that provide cloud-based email services (such as Gmail or Hotmail) also would be deemed to be "in possession" of all data attached to their users' email messages or stored in their users' accounts. Thus, to comply with BIPA, those providers would have to scan users' messages for biometric data; identify the people from whom that data was collected, or at least identify their state of residency; and then delete emails subject to BIPA, notwithstanding the wishes of the senders and recipients. That is an impossible burden that BIPA's authors never intended. *See Zellmer v. Facebook, Inc.*, No. 18-cv-01880, 2022 WL 976981, at *5 (N.D. Cal. Mar. 31, 2022) (noting the "Illinois Supreme Court's determination that BIPA should not impose extraordinary burdens on businesses"). And equally important, imposing that burden on email providers and others would thoroughly undermine the privacy interests of consumers by forcing providers to review and even destroy consumers' private data and communications.

"an active step to collect, capture, purchase, or otherwise obtain biometric data." *Id.*; *see also Jones v. Microsoft Corp.*, No. 1:22-cv-03437, 2023 WL 130495, at *3 (N.D. Ill. Jan. 9, 2023) (joining "many other judges" and holding that collection requires an "active step").

Ms. Redd does not allege that AWS took any "active step[s]" to collect her data. Indeed, she does not even allege AWS knew Wonolo collected her data. And Ms. Redd certainly does not allege that AWS played any role, active or otherwise, in Wonolo's decision to collect, analyze, and store her data. To the contrary, Ms. Redd alleges only that AWS acted as a passive, back-end service provider, while Wonolo determined what data to collect, when to collect it, and what to do with it. *See, e.g.*, Compl. ¶¶ 3, 5, 7. And, once more, it is worth noting that Ms. Redd's allegations are entirely consistent with AWS's Customer Agreement, which states that AWS customers like Wonolo "are solely responsible for the development, content, operation, maintenance, and use of [their] Content." Spear Decl., Ex. C (AWS Customer Agreement) ¶ 4.2.

Other courts have dismissed Section 15(b) claims where, as here, a plaintiff alleges only that a defendant acted as a third-party technology or service provider, not the collector of data. *See, e.g.*, *Jones*, 2023 WL 130495, at *2 (merely providing a "cloud computing storage platform" did "not constitute an active step or affirmative act"); *Jacobs*, 2021 WL 3172967 at *3 (dismissing Section 15(b) claim where the defendant was not the "active collector" but rather "merely provided the cameras" that another entity allegedly used to collect biometric data); *Namuwonge*, 418 F. Supp. 3d at 286 (similar); *Bernal v. ADP, LLC*, No. 2017-CH-12364, 2019 WL 5028609, at *1–2 (Ill. Cir. Ct. Aug. 23, 2019) (similar). This Court should do the same.[9]

Like her interpretation of "possession," Ms. Redd's interpretation of "collection" leads to "absurd, inconvenient, [and] unjust consequences" that this Court must avoid. *Solon*, 236 Ill. 2d at 441. Section 15(b) provides that a private entity may not collect biometric data from Illinois residents unless it first provides detailed notice and obtains written consent. *See* 740 ILCS

[9] One court has seemed to hold that Section 15(b) may apply to third-party service providers that merely store biometric data. *See Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 779 (N.D. Ill. 2020). AWS respectfully submits that *Figueroa* was wrongly decided, including because it fails to explain how passive storage, without more, amounts to active collection.

14/15(b). But Ms. Redd does not explain how AWS and similarly situated cloud-service providers could comply with those notice-and-consent requirements with respect to data they store on behalf of their customers. And for good reason: they simply could not do so. Again, AWS does not interact with Wonolo's end users, and it is contractually prohibited from "access[ing] or us[ing]" customer content, Spear Decl., Ex. C (AWS Customer Agreement) ¶ 3.2. It follows that AWS does not know and cannot know when its customers, including Wonolo, are collecting *biometric* data, let alone when they are collecting such data from *Illinois residents*. AWS therefore cannot provide prior notice to, and obtain prior consent from, its customers' end users in Illinois. To hold otherwise—that is, to construe BIPA to mean that back-end service providers like AWS are "required to provide notice to, and obtain consent from," end users "who [are] for all practical purposes total strangers"—would be "patently unreasonable." *Zellmer*, 2022 WL 976981, at *3–4.

Simply put, and for obvious reasons, it is not feasible for AWS to identify, notify, and obtain consent from all its customers' Illinois end users. Even if it was possible in theory, it would be hugely burdensome in practice, contrary to the legislature's intent. *See id.* at *5 (according to the Illinois Supreme Court, "BIPA should not impose extraordinary burdens on businesses"). Fortunately, nothing in BIPA imposes such impossible demands. Section 15(b) applies only "where a business ha[s] at least some measure of knowing contact with and awareness of the people subject to biometric data collection." *Id.* at *4. That is not the case here.

3. Ms. Redd alleges no facts showing that AWS "profited" from her data.

Ms. Redd's Section 15(c) claim fails for the additional reason that, even taking all the facts in the Complaint as true, she fails to adequately allege that AWS "profit[ed]" from her biometric data within the meaning of BIPA. 740 ILCS 14/15(c).

Ms. Redd's Section 15(c) theory boils down to the proposition that AWS used data about her face to "enhance"—i.e., to train, develop, and improve—"[AWS's] machine learning and AI technology programs, including . . . Rekognition." Compl. ¶ 44. But that profiting-by-training theory does not state a valid claim under Section 15(c).

Section 15(c) exclusively "regulates transactions with two components: (1) access to biometric data is shared or given to another; and (2) in return for that access, the entity receives something of value." *Vance v. Microsoft Corp.*, 534 F. Supp. 3d 1301, 1307 (W.D. Wash. 2021). Ms. Redd alleges no such transaction. Instead, she alleges only that AWS used her biometric data to train Rekognition and other (unidentified) services. *See* Compl. ¶ 44. That is not enough, however, because using biometric data to *train* an algorithmically-powered service like Rekognition does not entail *sharing* that biometric data with users of the service. As one court recently explained in rejecting a similar Section 15(c) claim:

> Plaintiffs' complaint is rife with allegations [about] how Amazon built its Rekognition Software [using] Plaintiffs' biometric information. But the Court agrees that nothing in the pleadings indicate[s] that the biometric information is being directly sold to any third party. Rekognition is [allegedly being sold to third parties], but Rekognition in and of itself is a set of algorithms. . . . *The Court does not find that a set of algorithms created using biometric information, but not containing any biometric information itself falls under section 15(c)*. A database is different from an algorithm. Databases generally contain actual information. Whereas, an algorithm [like Rekognition] is derived from a set of information but does not store the information it was derived from.

Hogan v. Amazon.com, Inc., No 21 CH 02330, Mem. Op. and Order at 3-4 (Ill. Cir. Ct. Dec. 6, 2022) (emphasis added) (attached as Exhibit G to the Spear Declaration). Thus, to adequately allege a Section 15(c) claim, Ms. Redd must "plead some facts leading to the inference that [her] 'biometric data is itself so incorporated into [Rekognition or other AWS products] that by marketing the product[s], [AWS] is commercially disseminating [her] biometric data.'" *Id*. at 4 (quoting *Vance v. Amazon.com, Inc.*, 534 F. Supp. 3d 1314, 1324 (W.D. Wash. 2021)). Ms. Redd alleges no such facts, nor could she. Her Section 15(c) claim must be dismissed.

4. Ms. Redd alleges no facts showing that AWS "disclosed" her data.

Ms. Redd's Section 15(d) claim also fails for an additional reason, namely, because Ms. Redd does not adequately allege that AWS disclosed her biometric data to anyone. At best, Ms. Redd asserts—in conclusory fashion—that AWS "disclosed, or otherwise disseminated [her] and putative class members' biometric data to other Amazon entities and subsidiaries,

AWS customers, and likely others." Compl. ¶ 51. But she does not offer any facts in support of that barebones (and false) assertion. She does not, for example, identify a single entity to which AWS allegedly disclosed her biometric data. Nor does she even try to explain why AWS would disclose her data. Further, the limited AWS conduct that Ms. Redd *does* allege—i.e., providing back-end storage and software services to Wonolo, *see* Compl. ¶¶ 3, 5–7, 39–42—does not in any way support the inference that AWS "systematically and automatically discloses, rediscloses, or otherwise disseminates" her biometric data. *Id.* ¶ 117.

In short, Ms. Redd offers nothing more than "conclusory allegations of disclosure, which merely parrot BIPA's statutory language." *Horn v. Method Prods., PBC*, No. 21 C 5621, 2022 WL 1090887, at *3 (N.D. Ill. Apr. 12, 2022) (dismissing Section 15(d) claim on those grounds). The Court could and should dismiss Ms. Redd's Section 15(d) claim for that reason. *See, e.g.*, *Carpenter v. McDonald's Corp.*, 580 F. Supp. 3d 512, 519 (N.D. Ill. 2022) (so holding).

5. AWS complied with BIPA's requirements.

Finally, even if Ms. Redd could overcome all the obstacles above, her claims would nevertheless fail because AWS complied with BIPA.

No statute requires the impossible. Accordingly, several courts have held that back-end service providers that do not interact with their customers' end users—like AWS—may comply with BIPA by contractually requiring their customers to comply with BIPA. *See Figueroa*, 454 F. Supp. 3d at 783 (explaining that a service provider "could have complied" with BIPA by requiring its customers "as a contractual precondition of using [the provider's] biometric timekeeping device, to agree to obtain their employees' written consent to [the provider] obtaining their data"); *see also Ronquillo v. Doctor's Assocs., LLC*, No. 21 C 4903, 2022 WL 1016600, at *3 (N.D. Ill. Apr. 4, 2022) (same) (citation omitted); *Guszkiewicz v. Beelman Truck Co.*, No. 2021L001248, Report of Proceedings at 19:16, 21–24 (Ill. Cir. Ct. Nov. 2, 2022) (holding that provider of biometric security cameras "satisfied [its] obligations under" BIPA by contractually requiring its customer to comply with the law, and observing that the Court did not "know how else" the provider could comply) (attached as Exhibit H to the Spear Declaration).

Under AWS's Service Terms, all AWS customers who use Rekognition (including Wonolo) are contractually required to "provid[e] legally adequate privacy notices to End Users" (including Ms. Redd). Spear Decl., Ex. D (AWS Service Terms) ¶ 50.4. Similarly, all such customers are required to "obtain[] necessary consent" and comply with other legal requirements, including for securing and deleting data. Ms. Redd has not alleged that AWS could have done anything more or different to comply with BIPA. Her claims fail for that reason, too.

CONCLUSION

For the foregoing reasons, AWS respectfully requests that the Court dismiss Ms. Redd's Complaint. Further, because Ms. Redd's claims cannot be cured by repleading, the Court should dismiss the Complaint with prejudice. *See Maron v. Am. Enter. Bank*, No. 21-2773, 2022 WL 807379, at *3 (7th Cir. Mar. 16, 2022).

Dated: January 17, 2023

AMAZON WEB SERVICES, INC.

By: */s/ Ryan Spear*
Ryan Spear

Ryan Spear
Nicola C. Menaldo
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000
Fax: 206.359.9000
Email: RSpear@perkinscoie.com
Email: NMenaldo@perkinscoie.com

Kathleen A. Stetsko
Perkins Coie LLP
110 N Upper Wacker Dr Suite 3400,
Chicago, IL 60606
Telephone: 312.324.8400
Fax: 312.324.9400
Email: KStetsko@perkinscoie.com